



## A Survey of False Alarm Protocol for Mobile Ad-hoc Networks

**Dr. S. Parryselvam**

M.E.,Ph.D., Associate Professor,  
Manakula Vinayagar Institute of Technology,  
Madagadipet, Pudhucherry, India

**K. Yazhini**

M.tech Student, Dept of Computer Science,  
Manakula Vinayagar Institute of Technology,  
Madagadipet, Pudhucherry, India

---

**Abstract**— *with the enlargement of the network size and application scope of mobile ad hoc networks, the variety and number of security needed by such protocols become more and more efficient. Furthermore, in this mobility environment, malicious nodes offering different services like deleting, rerouting, modifying data and node may leave the network any time due to absence of centralized administration. False alarm protocol becomes a new task of mobile ad hoc network. Producing alarm when malicious detection is crucial feature for the usability of mobile ad hoc networks. In this paper, we survey the researches of recent years on False alarm Protocol. Moreover, we analyze and compare these protocols. Based on the analysis, further research issues that still need investigation are listed.*

**Keywords**— *MANET, AODV, DSR, RSS*

---

### I. INTRODUCTION

In recent years, mobile ad hoc networks have been paid more attention due to their characteristics of highly dynamic, multi-hop, infrastructure-less and ease of formation. Especially, mobile ad hoc network have attracted more applications in specialized fields or relief scenarios such as battlefields, emergency services, disaster recovery during flood or earthquake, multi-hop extension for the existing wired or wireless networks etc. With the spread of the applications of mobile ad hoc networks, the number and variety of services provided by mobile ad hoc networks are continuously increasing. How to manage and control services of detecting malicious as to improve the usability of network becomes a new target of mobile ad hoc network. In the dynamic environment of mobile ad hoc network, malicious nodes offering different services like deleting, rerouting, modifying data and node may leave the network any time due to absence of centralized administration. Efficient and timely False alarm protocol becomes a prime task of intrusion management of mobile ad hoc network, a prerequisite for good utilization of packets on the network, and a crucial feature for the usability of mobile ad hoc networks. There have been intensive research efforts and extensive applications in the field of False alarm of most wired networks or some wireless networks.

#### The Basic Concepts of False Alarm Protocol

A false alarm protocol, also called alert alarm, is erroneous report of presence of malicious node in network, causing unnecessary changes where they are not needed. False alarms may occur when the nodes in network plays as selfish.

#### Classification of False Alarm Protocols in Mobile Ad Hoc Networks

- 1) Infrastructure - Based network: Wireless mobile networks usually been based on the cellular concept and depend on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the stable network infrastructure where false alarm will be generated from base station if any malicious detected.
- 2) Infrastructure less network: In infrastructure less approach there is no central administration for the entire network. The mobile wireless network is infrastructure less in manner commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing stationary network infrastructure. Here false alarm protocols used to detect the fault occur in network.

### II. RELATED WORK

In this section we provide extensive description of the existing false alarm protocols, which are grouped according to the taxonomy, defines in the introduction of this paper.

#### An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs

In this paper<sup>[1]</sup> general routing protocols for MANETs are designed based on the assumption that the nodes in network are cooperative with each other. However, due to the open structure and battery-based energy, misbehavior of node may exist. Such routing misbehavior is selfish nodes that will participate in the route discovery and maintenance processes but decline to forward data packets. In this paper, we propose the 2\_ACK scheme that provides service as an add-on technique for routing schemes which used to detect routing misbehavior and to mitigate their adverse effect. The goal of the 2\_ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. A fraction of the received data packets are acknowledged in the 2\_ACK scheme that used to to reduce additional routing overhead.

### **Handling Selfishness in MANETs**

In this paper<sup>[2]</sup>, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes in mobile ad hoc network. These selfish nodes could then reduce the overall data accessibility in the network along with an increase in query delay. So many people have worked on this selfish node problem, and proposed several methods to detect these selfish nodes. This paper provides a survey on different methods used to detect selfish nodes in MANETs. It also provides an overview on data replication in a mobile ad hoc network, and certain methods to handle selfishness occurring in this replica allocation process. It is being proposed to use a combined credit risk and collaborative watchdog method to improve the network performance by detecting such selfish nodes within a reduced time period.

### **Detecting Selfish Nodes in MANETs**

In this paper<sup>[3]</sup>, every node in it acts as a router as well as end-system and hence each node in MANET is allowed to move freely which makes routing difficult. Most of the MANET routing algorithms like AODV and DSR assume that every node will forward every packet it receives. Source node will relay packets to the destination node through the intermediate nodes. However, misbehaviour of the selfish nodes is a common phenomenon in MANET. These nodes use the network and its services and do not provide any services to intermediate nodes in order to save energy such as battery, CPU Power and band-width for relaying data from other nodes and reserve for themselves. These selfish nodes will degrade the performances of wireless ad hoc networks. However, we can identify the selfish nodes by modifying the original AODV and DSR routing algorithms. In this thesis, we proposed a time based scheme for identifying selfish nodes.

### **Derivative threshold actuation for single phase wormhole detection with reduction false alarm rate**

In this paper<sup>[4]</sup>, Communication in mobile Ad hoc networks is completed via multi-hop ways. Owing to the distributed specification and restricted resource of nodes, MANET is a lot prone to wormhole attacks i.e. wormhole attacks place severe threats to each Ad hoc routing protocol and a few security enhancements. Thus, so as to discover wormholes, totally different techniques are in use. In all those techniques fixation of threshold is merely by trial & error methodology or by random manner. Conjointly wormhole detection is in twin part by putting the nodes that is higher than the edge in a suspicious set, however predicting the node as a wormhole by using some other algorithms. Our aim in this paper is to deduce the traffic threshold level by derivational approach for identifying wormholes in a very single phase in relay network having dissimilar characteristics.

### **Detection of false alarm in handling of selfish nodes in MANET with congestion control**

In this paper<sup>[5]</sup>, the mobile nodes will have the characteristics of mobility and constraints in resources in mobile ad hoc network. Since, the mobility is high, the nodes may move randomly and fast, which lead to network Partitioning. The resource constraints lead to a big problem as decrease in performance and the network partitioning leads to poor data accessibility. To improve the data accessibility, we have proposed several data replication techniques. Most of the users at different places assume that mobile nodes co-operate fully in terms of sharing their memory space. But some nodes may decide as not to co-operate with others or partially co-operate with other nodes. The behavior of these selfish nodes leads to decrease in over all data accessibility of the network. We have explored the impression of selfish nodes in a MANET from the perspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation. The replica will be allocated using specific SCF tree concept. An alarm will be raised based on the selfish behavior of overall nodes called overall selfishness alarm. But the alarm will also be initiated because of network disconnections too but it seems and treated as overall selfishness alarm, it will affect the overall performance of the network. The concept of this paper deals with detection of false alarm as differentiated from overall selfishness alarm and to inform the other nodes at route as exactly where the disconnections occur to select the next best alternative path and also to increase the performance with increased congestion control. Detection of attacker node in the network and should be informed to all others in the network.

### **Detection of False Alarm in Handling of Selfish Nodes in Mobile Ad Hoc Networks**

In this paper,<sup>[6]</sup> A mobile Ad Hoc network is a collection of mobile nodes. They do not have any existing infrastructure and they do not have any centralized administrator. So the MANET is self-creating, self organizing and self-administrative wireless network. In MANET each node acts as router. In practice some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and bandwidth for retransmitting the data of other nodes. They will preserve the resources for their own use. Several data replication techniques have been proposed to minimize performance degradation. Most of them assume that all mobile nodes collaborate fully in terms of sharing their memory space. In reality, however, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes. These selfish nodes could then reduce the overall data accessibility in the network.

### **False Node Detection Algorithm in Cluster Based MANET**

In this paper<sup>[7]</sup>, Mobile Ad hoc network are collection of mobile nodes that can dynamically form temporary networks, it is necessary to bring the smart technologies in the Ad hoc network environment. Huge amount of time and resources are wasted while travelling due to traffic congestion. The idea behind clustering is to group the network nodes into a number of overlapping clusters. In the clusters of MANET The resource constraints leads to a big problem as

decrease in performance and the network partitioning leads to poor data accessibility due to false and selfish node. In our proposal the MANET area has been split into a number of size clusters having cluster head and storage capability according to connectivity degree, RSS (relative signal strength) as per the cluster formation algorithm given. In this cluster architecture we try to find false node inside clusters of MANET using a modified algorithm and try to remove them.

### **A Cooperative Intrusion Detection System for Ad Hoc Networks**

In this paper<sup>[8]</sup>, MANETs are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. So we report our progress in developing intrusion detection (ID) capabilities for MANET. Building on our prior work on anomaly detection, we investigate how to improve the anomaly detection approach to provide more details on attack types and sources. For several well-known attacks, we can apply a simple rule to identify the attack type when an anomaly is reported. In some cases, these rules can also help identify the attackers. We address the run-time resource constraint problem using a cluster-based detection scheme where periodically a node is elected as the ID agent for a cluster. Compared with the scheme where each node is its own ID agent, this scheme is much more efficient while maintaining the same level of effectiveness.

### **Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm**

In this paper<sup>[9]</sup>, Mobile Ad hoc networks are susceptible to several types of attacks due to their open medium, lack of Centralized monitoring and management point, dynamic topology and other features. Many of the intrusion detection techniques developed on wired networks cannot be directly applied to MANET due to special characteristics of the networks. However, all such intrusion detection techniques suffer from performance penalties and high false alarm rates. In this paper, we propose a novel intrusion detection method by combining two anomaly methods Conformal Predictor k-nearest neighbor and Distance based Outlier Detection (CPDOD) algorithm. A series of experimental results demonstrate that the proposed method can effectively detect anomalies with low false positive rate, high detection rate and achieve higher detection accuracy.

### **Eliminating Selfishness to Improve Replica Allocation over MANET's**

In this paper<sup>[10]</sup>, Mobile ad hoc networks are formed dynamically due to autonomous system of mobile nodes that are connected through wireless links without using an existing infrastructure or centralized administration. We have explored the impression of selfish nodes in a MANET from the perspective of replica allocation and developed selfish node detection algorithm that considers the partial selfish node and fully selfish node as selfish replica allocation. Some mobile nodes decided not to cooperate with other mobile nodes and simply aim to save its resources to the maximum while using the network to forward its own packets, these types of mobile nodes are called "Selfish Nodes" this misleading is very common in ad hoc network because of its configuration setup. These nodes could be detected and excluded from the cooperative portion of the network, as they only consume resources but don't contribute to the infrastructure. In existing methods, there are no steps to handle false alarms and efficient detection of selfish nodes. In this paper, a new mechanism that minimizes the problem of selfish nodes with the help of Credit risk and Brain trapping function Model. Including Degree of selfishness in allocating replicas will considerably reduce communication cost and produce high data accessibility.

## **III. CONCLUSION**

In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various False alarm methods to find selfish node in Manet on the basis of above mentioned performance metrics. The result after analysis has concluded and suggestion of mine is analyzing selfish node by using FAREP protocol is best when compared to above studied performance metrics.

## **REFERENCES**

- [1] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." *Mobile Computing, IEEE Transactions on* 6.5 (2007): 536-550.
- [2] Gayathry S S1, RNgaur2."Handling Selfishness in MANETs – A Survey", Vol. 3, Issue 11, November 2014.
- [3] Bathi Srikanth "Detecting Sel\_sh Nodes in MANETs", June 2014.
- [4] K.Aathi Dharshini1 C.Susil Kumar2 E.Babu Thirumangai Alwar3."Derivative Threshold Actuation For Single phase wormhole detection with reduction false alarm rate", Vol.5, No.1/2/3, May 2014
- [5] Ms. I.Shanthi1 and Mrs. D. Sorna Shanthi2."Detection of false alarm in handling of selfish nodes in MANET with congestion control", Vol. 10, Issue 1, No 3, January 2013.
- [6] Karthik M1 Jyothish K John2 Leenu Rebecca Mathew3 Tibin Thomas4."Detection of False Alarm in Handling of Selfish Nodes in Mobile Ad Hoc Networks", Vol. 1, Issue 10, 2013.
- [7] Gaurav, Naresh Sharma Himanshu Tyagi."False Node Detection Algorithm in Cluster Based MANET", Volume 4, Issue 2, February 2014.
- [8] Yian Huang Wenke Lee ."A Cooperative Intrusion Detection System for Ad Hoc Networks", Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages 135-147,2003.

- [9] Farhan Abdel-Fattah Zulkhairi Md. Dahalin Shaidah Jusoh .”Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm”, IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.
- [10] Yugandhara Bhalkar, Ujwala Chaskar, Vanashri Chaudhari, Chandrashekhar, Girigosavi.”Eliminating Selfishness to Improve Replica Allocation over MANET’s” , Volume 4, Issue 10, October 2014.
- [11] Y. Xiao, X. Shen, and D.-Z. Du .“A Survey on Intrusion Detection in Mobile Ad Hoc Networks”, (Eds.) pp. 170 – 196 °c 2006 Springer.
- [12] “S.Prabhavathi1 Ms.R.Bharathi2 .”Identifying and handling of false alarm in selfish replica” , Volume 5, Issue 2, February-2014 375
- [13] P.BakeyaLakshmi, Mrs.K.Santhi .”A survey on intrusion detection on MANEt”, Volume 1, Issue 5, October-2012.
- [14] K.Aathi Dharshini1 C.Susil Kumar2 E.Babu Thirumangai Alwar3.”Derivative threshold actuation for single phase wormhole detection with reduced false alarm rate” , Vol.5, No.1/2/3, May 2014.